The method by using user-defined ACL to match the length of packets in the H3C S3610/5510 Switches

岳斌 2009-02-09 发表

The method by using user-defined ACL to match the length of packets in the H3C S3610/5510 Switches

I Network topology

No

II Description of the problem

If you want to classify the data flow based on the length of packets, the basic, advanced and ? ethernet frame header ipv4 ACL could not make this requirement realized. But we could use another type of ACL which is supported in the H3C S3610/5510 switches.

III Process analysis:

The User-defined ACL, based on customized information, you can specify which bytes starting from the Layer 2 header or IP header should match the user-defined string. User-defined ACLs are numbered in the range 5000 to 5999.The format of creating a rule is as follows.

rule [*rule-id*] { **deny** | **permit** } [{ { **ipv4** | **ipv6** | **l2** | **l4** | **start** } *rule-string rule-mask offset* }&<1-8>] [**time-range** *time-name*]

Parameters description:

rule-id: User-defined ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

ipv4: Sets the offset from the beginning of the IPv4 header.

ipv6: Sets the offset from the beginning of the IPv6 header.

l2: Sets the offset from the beginning of the Layer 2 frame header.

l4: Sets the offset from the beginning of the Layer 4 header.

start: Sets the offset from the beginning of the outmost header.

rule-string: Defines a match pattern in hexadecimal format. Its length must be a multiple of two.

rule-mask: Defines a match pattern mask in hexadecimal format. Its length must be the same as that of the match pattern.

offset: Offset in bytes at which the match operation begins.

&<1-8>: Indicates that up to eight match patterns can be defined in the rule.

time-range time-name: Specifies the time range in which the rule can take effect. The time-name argument is a case-insensitive string of 1 to 32 characters. The name must begin with an English letter and cannot be all to avoid confusion.

IV Solution

An example for matching accurate length of the packets which is 1200 bytes. The configuration of ACL is as follows.

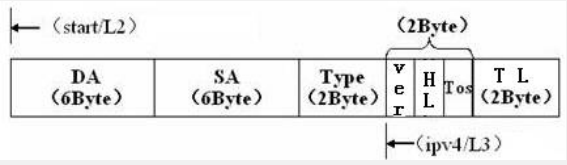
[H3C] acl number 5000

[H3C-acl-user-5000] rule permit start 04B0 ffff 16

or

[H3C-acl-user-5000] rule permit l3 04B0 ffff 2

Description of the above commands:



From above picture, if you choose "start" or "L2", that means offset of 16 bytes backward from the starting of ethernet frame is the total length of the starting of the packet ."04B0" is the hexadecimal express of 1200 and "ffff" expresses an exact match with "04B0" field of the packet.

If you choose "ipv4" or "L3", that means offset of 2 bytes backward from the starting of layer 3.

An example for matching length range of the packets which is 1200<=length<=1280 bytes. The configuration of ACL is as follows.

[H3C] acl number 5000

[H3C-acl-user-5000] rule permit start 04B0 fff0 16
Description: The rule matches the packets whose length ranges from 1200 to 1215,th at is,1200<=length<=1215.
Binary express of 1199 is 0000 0100 1010 1111, the hexadecimal is 04AF.
Binary express of 1200 is 0000 0100 1011 0000, the hexadecimal is 04B0.
Binary express of 1215 is 0000 0100 1011 1111, the hexadecimal is 04BF.
The previous 12 bits are the same in the range of 1200 ~ 1215,so by adjusting the m ask of "1" number to match the packets of the scope, that is, the pre-12 bits are all th e "1" which equals to "fff0" in hex.
[H3C-acl-user-5000] rule permit start 04C0 ffc0 16
Description: The rule matches the packets whose length ranges from 1216 to 1279,th at is,1216<=length<=1279.
Binary express of 1216 is 0000 0100 1100 0000, the hexadecimal is 04C0.
Binary express of 1279 is 0000 0100 1111 1111, the hexadecimal is 04FF.
Binary express of 1215 is 0000 0100 1011 1111, the hexadecimal is 04BF.
The previous 10 bits are the same in the range of 1216 ~ 1279,so the pre-10 bits are all the "1" which equals to "ffc0" in hex.
[H3C-acl-user-5000] rule permit start 0500 ffff 16
Description: The rule matches the packets whose length is 1280.